# Section 9

# SYSTEMS MANAGEMENT

## Contents



## General Information

Similar to support systems, systems management is not considered an independent subtopic of PSSs. Nevertheless, systems management is important and merits separate discussion to ensure that sufficient management planning, direction, and control processes are established and are adequately addressed during the inspection.

Management has the responsibility to ensure that security interests are adequately protected and that the levels of protection for particular interests are provided in a graded fashion in accordance with potential risks. In order to meet this responsibility, management performs a number of activities, including:

- Developing plans that include goals, objectives, and responsibilities for every aspect of physical protection
- Developing and implementing procedures and policies, considering site-specific conditions, that fulfill DOE requirements
- Providing adequate resources to include personnel (plus training), equipment, and facilities to meet the requirements contained in the procedures and policies
- Defining organizational and individual responsibilities (including accountability for performance)
- Performing management oversight activities such as self-assessments to identify areas that do not meet DOE policy requirements
- Monitoring the status of programs and policy implementation
- Correcting all areas of non-compliance in a timely and efficient manner.

## Common Deficiencies/ Potential Concerns

### Line Management Responsibility for Safeguards and Security

**Insufficient Management Support or Oversight.** Frequently, DOE and facility operations and production managers place a high priority on meeting production or operational goals, and are reluctant to commit limited/ competing resources or to implement physical security measures that are inconvenient or that would impact production. While some reluctance is understandable, compliance with minimum protection requirements must be met, and an appropriate balance between security and operations and production must be attained. Without the support of senior managers, the security organization may not have the assets necessary to operate effectively and, consequently, may be unable to maintain adequate protection levels. It is incumbent on senior managers and personnel responsible for oversight activities to assure that a lack of

management support does not adversely impact the effectiveness of security programs.

**Lack of a Suitable Organizational Structure.** Occasionally, inspectors encounter an organizational structure where the person or group responsible for policy and procedures is not positioned high enough in the organization to ensure compliance. This problem most often occurs when one organizational element is responsible for policy development, while personnel responsible for implementation work for different elements. The situation gets worse when the management element common to the two groups is at too high an organizational level to deal with day-to-day issues effectively. Similarly, inspectors may encounter situations where the security organization has little control or influence over engineering and/or maintenance personnel responsible for PSS design or functioning. In such cases, the operations and production managers to whom these personnel report may place a low priority on security issues and, in extreme cases, simply ignore the security organization's needs.

**Responsibilities Not Specifically Assigned.** Frequently, facilities fail to document the organizations and persons responsible for PSS operations. Less commonly, they may fail to assign responsibility for some aspects of the operations at all. Not documenting responsibility assignments inevitably results in some operational functions "falling through the crack." Responsibility for every aspect of the program should be specifically assigned in writing first to an organization, and then to a specific position or person within that group.

**Inadequate Staffing.** Some facilities simply do not have enough staff to support PSS requirements. A related problem occurs when a facility's manager cannot effectively manage the program, either because there are too many people to supervise (excessive span of control), or because the manager has other duties that deflects attention from physical protection responsibilities. In some cases, the site may have adequate numbers of staff, but may have a non-optimal skill mix, resulting in shortages in certain areas and/or delays in performing certain functions.

## Personnel Competence and Training

**Inadequate Training.** Many PSS-related deficiencies found in DOE are attributable to inadequate training. Some organizations do not provide any formal training. They rely instead on an unstructured form of on-the-job training. They expect persons with security responsibilities to learn from other, more experienced individuals. Often, however, the experienced individuals themselves lack adequate training, so improper practices continue. In some cases, organizations make attempts at training, but develop and administer it using individuals unfamiliar with proper training techniques. This practice also results in inadequately trained persons performing key duties. Few organizations evaluate the competency of individuals with security responsibilities before allowing them to assume their assigned tasks. Even people who have completed a well-designed training program may not have adequately learned all aspects of their duties. If a training program exists, inspectors should focus on reviewing its effectiveness. If no training program exists, inspectors should devote additional attention to activities designed to determine the knowledge level of individuals who perform security functions (for example, interviews or knowledge tests).

## Comprehensive Requirements

**Inadequate Planning.** Frequently, during physical security planning, management does not give adequate consideration to, or overlooks, potential threats and/or adversary approaches regarded as unconventional. As a result, concerns that would otherwise be identified are often not adequately dealt with and are not addressed in the appropriate planning documents (for example, the SSSP and supporting VAs for Category I SNM facilities). During planning, it is important that managers consider the impact of conditions such as non-traditional ingress points (e.g., airborne intrusion) and thoroughly review the consequence of insider activity with emphasis on single point failure potential.

**Inadequate Implementation of Requirements.** More often than not, facilities develop policies and procedures that provide adequate guidance and direction for the protection of identified security interests. However, inadequate implementation of the requirements delineated in those documents frequently results in protection levels that are less than what was intended. The resultant impact of inadequate requirement implementation is more crucial in some areas than it is in others. For example, deviations from protection policies involving the protection of high-value non-classified equipment does not hold the same level of importance as those involving SNM. Areas where inadequate implementation is common and where resultant impacts can be significant include material surveillance, SNM transfers, emergency operations, protective force operations, and alarm response.

### Feedback and Improvement

**Inadequate Self-Assessment Process.** Not all facilities have implemented a comprehensive self-assessment program. Others lack the expertise to implement such a program effectively. Therefore, they rely on periodic security surveys to provide data for self-assessment of the local personnel security program. The lack of an effective self-assessment program can result in deficiencies going undetected and uncorrected for extended periods.

**Inadequate Corrective Action Plans.** This is somewhat common and potentially serious deficiency that can result in deficiencies not being corrected. Organizations frequently fail to effectively accomplish one or more of the following actions: (1) analyze (root cause and cost effectiveness) and prioritize deficiencies so that resources can be used to correct the most serious first, (2) establish a corrective action schedule with milestones so progress can be monitored and slippages identified early, (3) assign responsibility for completion to specific organizations and individuals, (4) continually update the plan as known deficiencies are corrected and new ones are identified, and (5) ensure that adequate resources are applied to correcting deficiencies. Frequently, facility managers devote their resources to "putting out brush fires" (that is, correcting the most recently identified deficiency instead of the most serious, and habitually correcting symptoms rather than the root causes of systemic deficiencies).

**Incomplete or Inadequate Deficiency Tracking Systems.** Tracking system inadequacy is a common and potentially serious deficiency often found in the management area. Tracking system problems can result in not correcting deficiencies in a timely manner, or not correcting them at all. The two most common problems found in tracking systems are incompleteness and inaccuracy. Often, the system is incomplete because supervisors or operators fail to list all deficiencies. They are inaccurate when corrective actions are shown as complete when they are not, or when they have not adequately dealt with the problem. Occasionally, inappropriate corrective action based on inaccurate tracking data creates new problems.

**No Root Cause Analysis of Deficiencies.** Another potentially serious management deficiency is the failure of organizations to determine the underlying cause of deficiencies. This usually results in the same deficiencies recurring. Many times, the organization corrects the surface problem or symptom rather than identifying and correcting the underlying cause—the root cause. If performed correctly, a root cause analysis may reveal the causes of errors (e.g., ambiguous procedures or insufficient training). Unless management accurately determines the root cause of identified deficiencies, it is likely that similar deficiencies will recur.

## Planning Activities

During planning, inspectors interview points of contact and review available documentation (for example, SSSP, procedures, self-assessments, survey reports, and other pertinent documents) to characterize the program. Inspectors should:

- Determine the organizational structure, including whether a central group establishes and monitors compliance with procedures. If

not, determine how many separate points of authority for the program exist among the various organizational elements.

- Review organizational charts and determine the names of all persons with PSS supervisory and management authority.

- Determine how PSS policy and procedures are promulgated and distributed.

- Determine how the self-assessment program functions, including the frequency of self-assessments, who has overall authority for the program, and who actually performs the self-assessments. Focus on determining whether the self-assessment program provides independent oversight of PSSs, or whether it is conducted by the same persons who operate the programs being assessed.

Once inspectors understand the structure of the program, they should determine which organizations and program elements will be reviewed in more depth during the inspection, and which individuals will be interviewed. At large facilities, it is not practical to inspect all systems in the same depth or to interview all individuals who perform systems related duties. In such cases, a representative sample may be selected for evaluation. Typically, inspectors will be covering other PSS subtopics as well as systems management for reasons of efficiency. Consequently, a variety of factors should be considered when selecting organizations to review. It is usually advisable to interview first-line managers with responsibility for the systems that are selected for performance tests. This ensures that the impact of any deficiencies identified during the reviews can be covered with managers during the management interviews. Frequently, the information gathered during the first few days of the inspection will influence the selection of managers to be interviewed. As program strengths and weaknesses are noted, the inspectors should modify their planned activities appropriately.

Inspectors review basic documentation and interview facility security and protective force representatives to determine how the protective force implements security-related procedures. Areas to review include patrols, repository checks, alarm responses, SNM transfers, emergency response, and training. Such reviews should be closely coordinated with the protective force topic team. Typically, the PSS team would focus on the protective force interface with security systems. The systems team would not normally attempt to evaluate the tactical capabilities of the protective force (for example, weapons-related skills or the ability to use cover and concealment).

## Data-Collection Activities

### Line Management Responsibility for Safeguards and Security

**A.** Inspectors should review the applicable planning documents that cover PSS (for example, SSSPs or other planning documents). Inspectors should devote particular attention to determining whether the planning documents are current; whether they appropriately identify the goals, objectives, responsibilities, and overall policies for all aspects of physical security systems; and whether they address all applicable security interests. Any special conditions or unique features of the site that are covered by exceptions or alternative approaches should be reviewed to determine whether the facility has documented the justification for the exceptions.

**B.** Interview security managers, including design and testing/maintenance supervisors, and review resource plans and budget documents. Elements to cover include:

- Whether goals and objectives are clearly defined

- Whether needs identified in the corrective action plan and strategic plan (if one exists) are reflected in budget documents

- How the PSS budgeting process functions

- Whether there is consistency between staffing plans and budget requests.

**C.** Inspectors should determine whether the organizational structure facilitates efficient

communication and positive working relationships between the various organizational elements, and between persons who deal with PSSs. It is important that the functional relationships between the various organizational elements be clearly defined, formally documented, communicated, and understood by all persons. One method useful for investigating the adequacy of the communications and interactions between organizational elements is to determine how the organizations interact with one another (for example, protective force and material control and accountability) when facility conditions change (for example, during material transfers between security areas).

**D.** Inspectors should determine whether the persons responsible for PSSs are in a position to ensure compliance. This may involve reviewing the facility's policies and procedures to determine whether the safeguards and security manager has the authority to enforce compliance and resolve issues identified during self-assessments or other similar activities.

Additionally, interviews with managers in the security department and operations and production departments should be conducted to determine whether the security organization has any problems getting the operations or production personnel to implement required procedures. If initial interviews indicate questions about the operations or production organization's commitment to implementing required security measures, inspectors may elect to conduct more detailed interviews (i.e., with individual vice managers) and document reviews to determine whether problems exist. This detailed review may involve examining findings identified in self-assessments, surveys, and inspections to determine whether corrective actions were implemented in a timely manner, or whether repeated memoranda from the security organization were necessary before the operations or production personnel took action. Other indicators of problems include a pattern of repeated deficiencies at the same location and "backsliding" (that is, implementing corrective actions after a deficiency is identified, and then discontinuing the corrective measures later, after the "heat is off").

**E.** Inspectors should determine how management communicates its goals and objectives and stresses the importance of PSS. Inspectors should determine what incentives are used to encourage good performance.

### Personnel Competence and Training

**F.** Inspectors may elect to review a sample of position descriptions of specific individuals who have responsibilities for PSS to verify that responsibilities are actually reflected at the individual's level. Inspectors can also review individual position descriptions and performance goals of technicians or other persons in the operations and production departments that conduct performance tests or perform maintenance functions to determine whether individuals are held accountable for their performance and whether good performance in PSS-related areas is included.

**G.** Inspectors should review actual versus authorized staffing levels for PSS positions to determine whether the program is operating short-handed. Inspectors must be especially watchful for non-PSS responsibilities being assigned to key program personnel, detracting from their ability to perform their PSS duties.

**H.** Inspectors should review training plans, course material, and training needs analysis; interview security staff, operations/production supervisors, and custodians; and/or observe training classes that address any aspect of security-related functions. This may include training of SPOs, custodians, operators, health physics staff, and other personnel who perform security-related functions. This is done to determine whether security-related concerns are understood by operations and field personnel — not only the security practice, but the reason for the practice. For example, the SPO responsible for monitoring a metal detector may have been given orders that all incoming personnel must clear the metal detector, but no mention of outgoing personnel was made. If the SPO does not fully understand the purpose of the metal detector (to prohibit the introduction of weapons and contraband **and** to prevent removal of SNM

or DOE property), the SPO may fail to have outgoing personnel clear the metal detector.

**I.** Inspectors should review training records and test scores and interview personnel who have received training to verify that training has been conducted as scheduled and that personnel attended courses as required. During interviews, the inspectors should ask facility personnel questions taken from facility tests as a means of determining the effectiveness of the training program. The inspectors may also request that personnel perform functions for which they have been trained (for example, test an alarm sensor, apply a tamper-indicating device, operate a handheld SNM detector). In this manner, the inspectors can observe the knowledge and skills of individuals and verify the training program effectiveness.

### Comprehensive Requirements

**J.** Planning – Airborne Protection. Inspectors should review the SSSP to determine whether airborne assault is considered in the site-specific threat. Document review and interviews should reveal whether an airborne threat is appropriate for the site (for example, if the only security interest at the site is a single piece of SNM weighing two tons buried in a solid piece of concrete 15 feet thick, the airborne threat may not be appropriate to the site). However, if the security interests are more attractive, smaller and more vulnerable, the inspection team should evaluate all airborne denial barriers and detection equipment.

If an airborne threat is credible, inspectors should review documents and interview security staff to determine the level of protection against airborne intruders. Items to check include whether:

- The airborne threat is addressed in the SSSP
- Helicopter barriers (for example, poles and rope systems) have been installed to protect priority targets
- An electronic detection system is used (for example, acoustic detectors or radar). If so, the methods for testing effectiveness should be reviewed.
- Other means of detecting airborne intrusion are available (for example, SPOs in exterior posts, and patrols).

Inspectors should also tour areas to determine the degree of protection against airborne threats. Items to note include:

- Potential landing sites that could be used by helicopters, gliders, parachutists, or fixed wing aircraft
- Likelihood of detecting intrusion (factors such as the size of the area, visual detection capability from guard posts, frequency of patrols, and general level of activity in the area should be considered)
- Effectiveness of any aircraft denial barriers, including susceptibility to defeat by covert means.

**K.** Planning – Insider Analysis. Inspectors should determine the vulnerability of high-security facilities (for example, those with Category I SNM or vital equipment) to possible insider actions, including:

- SPOs
- CAS operators
- Custodians
- Operators
- Supervisors
- Security technicians
- Maintenance personnel
- Health physics technicians
- Emergency response personnel (for example, firefighters).

This can be accomplished by reviewing VAs, interviewing personnel in various job categories, and systematically examining the job duties, responsibilities, and "privileges" of personnel in selected job categories (for example, possession of master keys, access to safe combinations, capability to place alarm systems in access mode). The inspectors should pay particular

attention to personnel who have access to SNM and who have numerous responsibilities (for example, material custodians who also test alarms, have safe combinations, and enter information into accountability systems). The inspectors should also look for possible single-point failures (for example, areas where the entire safeguards system would be ineffective if one element were to fail) and determine whether the elements possibly involved in such failures are vulnerable to insider sabotage.

**L.** Requirement Implementation – Material Surveillance Procedures. Inspectors should review documents such as the MC&A plan, operating procedures, and the SSSP; interview security staff, material custodians, operators, or other personnel who use or process SNM; and tour process areas to determine the methods used to provide surveillance of material that is not in secure storage. Material surveillance of SNM must be maintained within use and process areas. A two-person rule is a common method of implementing material surveillance at Category I or II areas. Custodial and administrative controls are generally used in Category III or IV areas.

The inspection team should pay particular attention to the means of providing material surveillance for SNM kept in process storage or staging areas. The inspectors should ensure that all practices are consistent with MC&A plan provisions and are effectively implemented.

The effectiveness of the two-person rule should be determined by reviewing and observing procedures. Inspectors should verify that procedures are developed for all areas and distributed to all personnel who must implement them. The procedures should clearly specify what is required (for example, constant visual contact, two persons in same room, or two persons in same vault). The means of enforcement of a two-person rule at MAAs or vault entrances can also be reviewed. Card-reader systems, SPO procedures, and double-lock systems are common methods for enforcing a two-person rule. In some areas, the inspectors may also review access logs to determine whether the two-person rule is implemented as required. The inspectors should attempt to observe implementation of the two-person rule and interview the material handlers or custodians to determine whether they understand and implement the requirements correctly. All of the aforementioned activities should be closely coordinated with the MC&A team as reflected in Section 10.

**M.** Requirement Implementation – SNM Transfer Procedures. Inspectors should identify:

- The SNM transfer paths, including offsite shipping and receiving and intrasite transfers; the category and classification of SNM transfers
- Specific portals used for SNM transfers and controls implemented at those portals by the operations, production, and health physics staffs, and by the material custodians and the protective force
- Escort procedures, including the number of armed SPOs that accompany Category I shipments
- Vehicles used for shipments, including special security features of vehicles (for example, remote-disable capability, hardened vehicle, locked-storage, delay features)
- Methods to assure that SNM is not secreted in non-SNM transfers and/or radioactive waste shipments.

Inspectors should observe SNM transfers to determine effectiveness and verify information collected during interviews and document reviews. Procedures at the shipping portal and/or receiving portal should be observed as well as the transfer route.

Once the inspectors have an operational understanding of the transfer procedures, they should evaluate the procedures for vulnerabilities or weaknesses. This can be accomplished using the "what if" approach (for example, What if the vehicle driver is the insider? Are there procedures that will prevent the driver from driving away with the material?).

**N.** Requirement Implementation – Emergency Procedures. Inspectors should review SSSPs,

standard operating procedures, emergency plans, post orders, and other documents; interview security managers, protective force supervisors, custodians, and operations/production supervisors; and tour use and process areas to determine:

- Methods used to ensure security of SNM during and following an emergency, including:
  - Evacuation alarms
  - Fire alarms
  - Criticality alarms
  - Medical emergencies
  - Radiation alarms
  - Toxic chemical situations.
- Requirements and conditions for post-evacuation SNM inventories
- Methods used to control evacuation, including SPO response, preplanned evacuation routes with barriers, post-evacuation personnel accounting, and post-evacuation patrols and searches
- Protective force procedures, including response plans
- Custodial procedures
- Operations/production procedures
- Health physics procedures.

Inspectors should verify information about emergency evacuations by observing facility tests or reviewing results of after-action reports (incident reports). For example, if evacuations have occurred, the inspectors can usually review incident reports and verify that an inventory was performed as required by site-specific procedures.

**O.** Requirement Implementation – Protective Force. Inspectors should interview security staff and protective force supervisors and review security plans and post orders to determine:

- Frequency of patrols of selected areas
- Duties and responsibilities (for example, check locks, check repositories, detect intrusion)
- Documentation of patrols (for example, logs and punch clocks)
- Requirements for repository checks.

Inspectors should review logs on classified repositories to verify that SPOs sign/initial logs as required by site-specific policy.

Inspectors on the PSS team need to know whether facility procedures include support by the protective force to adequately protect DOE assets according to facility plans and accepted risks. These patrols are normally a part of the security posture agreed to or directed by DOE. All of the aforementioned activities should be closely coordinated with the protective force team as reflected in Section 10.

**P.** Requirement Implementation – Alarm Response. Inspectors should interview security staff and protective force supervisors and review security plans and post orders to determine:

- Alarm response plans
- Alarm priorities
- Response times
- Number of responders.

Response actions for various alarms and conditions, including:

- Exterior intrusion alarms
- Interior intrusion alarms
- Tamper or line supervision alarms
- Duress alarms
- SNM monitor alarms
- Evacuation alarms
- Emergency response (for example, fire)
- Visual sighting of intruder.

- Methods for assessing, recording, and documenting alarms and/or response actions
- Tests conducted by the facility to verify response times or effectiveness.

Inspectors should review logs and/or incident reports to verify response times and actions. Such logs are usually maintained by the CAS and the protective force supervisors.

Inspectors should observe response procedures during routine activities or during facility tests and verify appropriate response actions.

Inspectors should validate the alarm response times to assure that the VA models accurately reflect the required delay times and security responses, and that security interests are adequately protected.

### Feedback and Improvement

**Q.** Most organizations have some type of central, integrated system to identify and follow the status of deficiencies identified during self-assessments, operations office surveys, and inspections. Inspectors should determine what system or systems are being used. Sometimes it is a comprehensive system that includes all safeguards and security-related deficiencies. Other times, each area, including personnel security, has a separate tracking system. Self-assessment programs are the key to effective management oversight of personnel security.

**R.** Inspectors should review the self-assessment program in detail. They should determine whether self-assessments are performed regularly and whether they review all aspects of the personnel security program. Selected self-assessment reports should be reviewed to determine whether root causes are identified when deficiencies are found. It is helpful to compare the results of facility self-assessments to inspection findings or other audit results to learn whether the self-assessments are equally as effective.

**S.** Inspectors should determine who actually performs the self-assessments. At the operations office this may be the security survey staff as they perform the annual survey. If the persons who actually perform personnel security functions conduct the self-assessments, there should be some form of independent verification or evaluation of the results. Inspectors should determine whether deficiencies identified during self-assessments are entered into a tracking system, and how corrective actions are selected and achieved.

**T.** Inspectors should determine whether an organization has a tracking system and how it operates. In conjunction with the survey program topic team, they should determine whether the tracking systems have a means of monitoring the status of all inspections, surveys, self-assessments, and other similar activities. Also, inspectors should determine whether there is a formal system to independently verify that corrective actions have been completed and that the original problem has been effectively resolved. Inspectors may elect to select a sample of personnel security deficiencies from several sources and determine whether they were entered into the tracking system. Finally, they can select a sample of deficiencies indicated as closed to verify that they have in fact been adequately corrected.

**U.** Inspectors should determine whether corrective action plans exist for deficiencies and whether deficiencies are analyzed and prioritized. They should determine whether schedules and milestones have been established, and whether specific responsibilities to ensure completion have been assigned down to the individual level. Inspectors should also determine whether root cause analyses are performed. If so, the inspectors should request documentation on root cause analyses for significant deficiencies listed in the tracking system and the rationale for the particular course of corrective actions chosen. As a related activity, inspectors may elect to review how resources required for corrective actions are introduced into the budget process.

**V.** Inspectors should review the role of DOE oversight by interviewing selected DOE security or survey managers to determine how DOE implements its responsibilities. Specific items to cover include how DOE reviews the contractor personnel security program functions on surveys, how DOE tracks the program status, and how DOE and the facility interact on a day-to-day basis. Additionally, key facility managers should be interviewed to gather their views on the same subjects.

This page is intentionally left blank.